



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,505	05/05/2006	Miodrag J. Mihaljevic	287806US8PCT	9441
22850	7590	09/16/2010	EXAMINER	
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P. 1940 DUKE STREET ALEXANDRIA, VA 22314			ZIA, SYED	
			ART UNIT	PAPER NUMBER
			2431	
			NOTIFICATION DATE	DELIVERY MODE
			09/16/2010	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com  
oblonpat@oblon.com  
jgardner@oblon.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/578,505	<b>Applicant(s)</b> MIHALJEVIC ET AL.	
	<b>Examiner</b> SYED ZIA	<b>Art Unit</b> 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 08 July 2010.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-9 and 11-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-9 and 11-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)                        | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

This office action is in response to amendment and remarks filed on June 24, 2010.

Claims 1-9, and 11-20 are pending for consideration.

#### ***Claim Rejections - 35 USC § 101***

1. Applicant amended the Claims. Previous rejection under 35 U.S.C. 101 has been withdrawn.

#### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 7, 2010 has been entered.

#### ***Response to Arguments***

Applicant's arguments filed on June 24, 2010 have been fully considered but they are not persuasive because of the following reasons:

Art Unit: 2431

Regarding Claims 1-9, and 11-12 applicants argued that the previously cited prior arts (CPA) [7,178,030)] neither describes nor suggest *"cellular automata random number generator of a second type for generating a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger than the first predetermined period," and "performing bit-to-bit mod2 sum of the first sequences and the second sequences."* Furthermore, cited prior art does not describe or suggest *"performing bit-to-bit mod2 sum of the first sequences and the second sequences"*.

This is not found persuasive. Applicant's arguments with respect to claims 1-9, and 11-20 have been considered but are moot in view of the new ground(s) of rejection.

The system of newly cited prior art (U.S. Patent No.: 7,571,200) clearly teaches a method to generate cellular automata based random number. This cellular automata-based random number generator is where an output of each cell of the cellular automata at time  $t$  is dependent on inputs from any cells of the cellular automata (including perhaps itself) at time  $t-1$ .

The system of cited prior art teaches multiple Cellular automata random number generator [204.sub.o to 204.sub.m-1, Fig.5] where the different selected bits of the multiple CA RNGs are combined with bits of selected stages of the LFSR RNG. A selected bit from one of the CA RNGs is provided to an XOR element, along with a bit from a selected stage of the LFSR RNG. For example, the bit from cell, from CA RNG 204.sub.j ( $0 \leq j \leq m-1$ ) and the bit from stage.sub.k of the LFSR are provided as input to XOR 206.sub.0.

In the system of newly cited prior art (Fig. 3) also disclosed a composite RNG with desirable random number properties and a desirable cycle length is constructed from a first RNG

Art Unit: 2431

with desirable random number properties and a second RNG that has a desirable cycle length but poor statistical properties.

As a result, the system of cited prior art does implement and teaches a method and apparatus of finite state machine for generating pseudorandom sequences with controllable period (Fig. 2-6 and col.4 line 12 to col.6 line 41).

Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that the cited prior art does claim or suggest the subject matter as recited in independent Claims and in subsequent dependent. Claims of the instant application and the instant application Claims are obvious variation of already claimed cited prior art. Accordingly, rejections for claims 1-9, and 11-20 are respectfully maintained.

### ***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-9, and 11-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2431

4. Regarding claim 1, 9, and 11: it's not clear to what does "to generate a second sequence with a second predetermined randomness lower than the first predetermined randomness;" means in the context of this claim. Examiner could find the description or definition of this term in the disclosure.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9, and 11-20 are rejected under 35 U.S.C. 102 (e) as being anticipated by Shackleford et al. (U. S. Patent 7,571,200) (hereafter Shackleford'200)

1. Regarding Claim 1 Shackleford teach and describe an apparatus for generating pseudorandom sequences comprising: a cellular automata random number generator of a first type configured to generate a first sequence with a first predetermined randomness and a first predetermined period;

a cellular automata random number generator of a second type configured to generate a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger than the first predetermined period; and

Art Unit: 2431

adders configured to perform bit-to-bit mod2 sum of the first sequences and the second sequences (Fig. 2-6 and col.4 line 12 to col.6 line 41).

2. Regarding Claim 9 Shackleford'200 teach and describe a method for generating pseudorandom sequences using cellular automata in a pseudorandom sequence generator comprising: generating, at a cellular automata random number generator of a first type, a first sequence with a first predetermined randomness and a first predetermined period; generating, at a cellular automata random number generator of a second type, a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger than the first predetermined period; and performing, at an adder, bit-to-bit mod2 sum of the first sequences and the second sequences (Fig. 2-6 and col.4 line 12 to col.6 line 41).

4. Regarding Claim 11 Shackleford'200 teach and describe a recording medium storing a computer program for causing a computer to execute a method for generating pseudorandom sequences using cellular automata, the recording medium wherein: the method includes generating a first sequence with higher randomness; generating a second sequence with predetermined lower bound on the period; and performing bit-to-bit mod2 sum of the first sequences and the second sequences (Fig. 2-6 and col.4 line 12 to col.6 line 41).

Art Unit: 2431

5. Claims 2-8 and 12-20 are rejected applied as above rejecting Claims 1, 9, and 10-11.

Furthermore, Shackleford'200 teach and describe a method for generating pseudorandom sequences using cellular automata, wherein:

As per claim 2, the cellular automata random number generator of a first type is two-dimensional cellular automata; the cellular automata random number generator of a second type is 2-by-L cellular automata; and summation results from the adders are outputted as the pseudorandom sequences (col.4 line 12 to col.6 line 16)

As per claim 3, further comprising: cellular automata random number generator of a third type configured to generate a third sequence, the cellular automata random number generator of a third type determines cell states based on a corresponding cell control word and/or a corresponding rule control word; wherein the cell control word is generated by the cellular automata of a second type; the rule control word is generated by the cellular automata random number generator of a first type; and the adders perform bit-to-bit mod2 sum of the first, the second and the third sequences (col.4 line 12 to col.6 line 41).

As per claim 4, the summation results from the adders are outputted as pseudorandom sequences (col.6 line 12 to line 52).

As per claim 5, further comprising: a first block configured to perform a nonlinear mapping on the summation results from the adders; and a second block configured to perform a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as the pseudorandom sequence (col.5 line 23 to col.6 line 41).

As per claim 6, each of the blocks includes at least one nonlinear function (col.5 line 23 to col.6 line 41).

Art Unit: 2431

As per claim 7, the second block for mapping includes at least one look-up table for nonlinear mapping based on the Latin squares (col.3 line 12 to line 33).

As per claim 8, a cryptographic processor for encrypting data using pseudorandom sequences; and a pseudorandom sequence generator for generating the pseudorandom sequences; wherein the pseudorandom number generator is configured to include the apparatus according to claim 1 (col.6 line 15 to line 52).

As per claim 12, the first sequence generated by the cellular automata random number generator of a first type satisfies the DIEHARD test (col.1 line 32 to line 48).

As per claim 13, the cellular automata random number generator of a first type generates two-dimensional cellular automata including 64 cells (col.3 line 50 to line 40).

As per claim 14, the cellular automata random number generator of a first type generates two-dimensional cellular automata arranged in an 8x8 array (col.3 line 50 to line 40).

As per claim 15, further comprising: a buffer configured to buffer results of the bit-to-bit mod2 sum (col.4line 54 to col.5 line 10).

As per claim 16, the adders output pseudorandom sequences with a controllable period (col.4 line 41 to col.5 line 10).

As per claim 17, the cellular automata random number generator of the third type includes a plurality of cell units (col.4 line 41 to col.5 line 10 and col.5 line 65 to col.6 line 13) .

As per claim 18, further comprising generating a key for cryptographic processing based on the generated pseudorandom sequences (col.6 line 15 to line 51).

As per claim 19, further comprising interfacing with an external device (col.3 line 34 to line 50).

Art Unit: 2431

As per claim 20, wherein the interfacing includes inputting information designating the key to be used and outputting encrypted text data based on the key (col.3 line 34 to line 50).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SZ

September 9, 2010

/Syed Zia/

Primary Examiner, Art Unit 2431